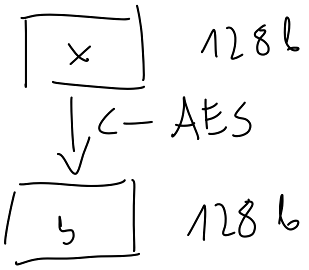
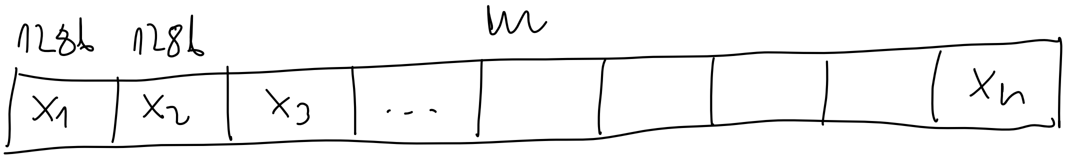
AES





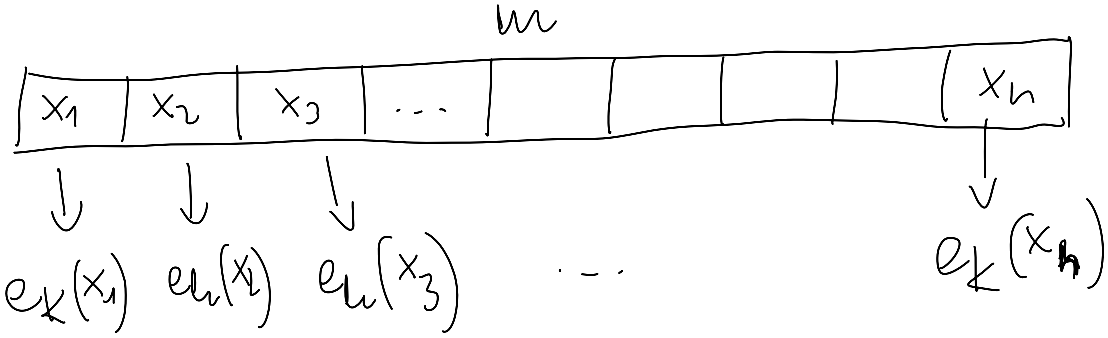
Tryby: ECB electronic codebook (NIE STOSOWAĆ)

CBC cipher block chaining

OFB output feedback

CFB cipher feedback

CTR counter



CBC

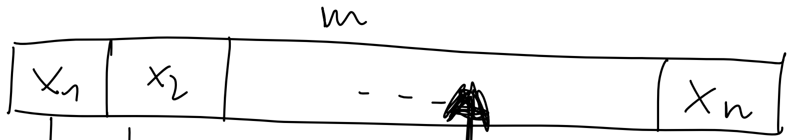
IV - initialization vector

1) długości równa dł. bloku

2) jawne

3) wyznaczany raz dla ustalonego klucza

4) losowany



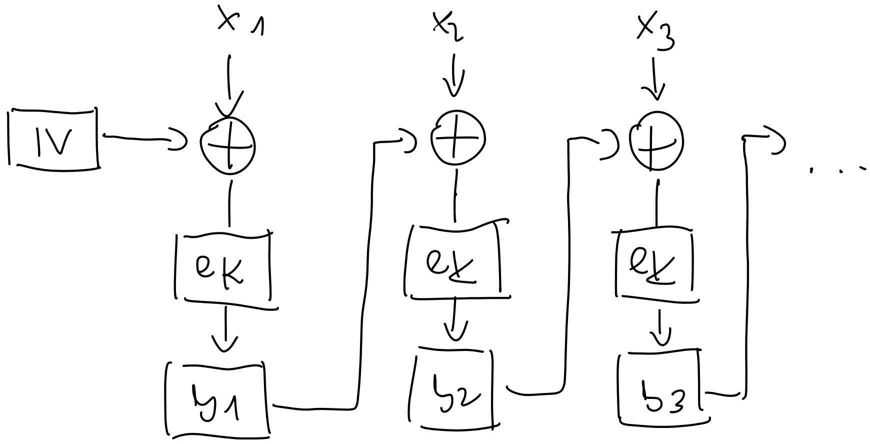
$y_0 = IV$

$y_1 = e_K(y_0 \oplus x_1)$

$y_2 = e_K(y_1 \oplus x_2)$

...

$y_i = e_K(y_{i-1} \oplus x_i)$



MAC - message authentication codes

OFB np. AES

$z_0 = IV$

$z_1 = e_K(IV)$

$z_2 = e_K(z_1) =$

$= e_K(e_K(IV))$

$z_3 = e_K(z_2)$

$\vdots$

$z_i = e_K(z_{i-1})$

$i \geq 0$

OTP

$\boxed{y_1 = z_1 \oplus x_1}$

$y_2 = z_2 \oplus x_2$

$\vdots$

$y_i = z_i \oplus x_i$

IV $\quad z_1, z_2, \dots$

$x_1 = y_1 \oplus z_1$

$\vdots$

$x_i = y_i \oplus z_i$

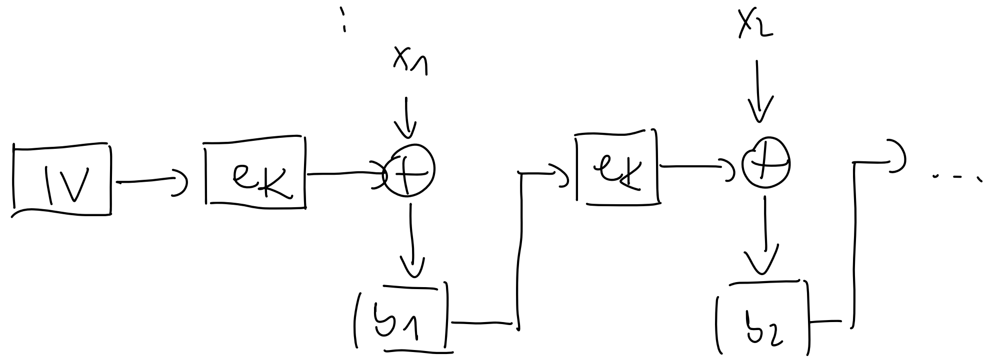
CFB

$y_0 = IV$

$z_1 = e_K(y_0) \rightarrow y_1 = x_1 \oplus z_1$

$z_2 = e_K(y_1) \rightarrow y_2 = x_2 \oplus z_2$

$\vdots$



CTR

ctr - licznik poczatkowy (dł. bloku, n bitów)

$T_1, T_2, \ldots$

$T_1 = ctr$

$T_2 = ctr + 1$

$T_3 = ctr + 2$

$\vdots$

$$T_i = ctr + i - 1 \mod 2^n$$

$$\left.\begin{aligned} z_1 &= e_K(T_1) \\ z_2 &= e_K(T_2) \\ &\vdots \\ z_i &= e_K(T_i) \end{aligned}\right\} \text{mogą być wyliczone równolegle}$$

$$y_i = x_i \oplus z_i \qquad \text{(OTP)}$$

$$\boxed{T_{158} = ctr + 158 - 1}$$

128b	128b	m	128b	64b
x_1	x_2	...	x_n	x_{n+1}

Padding

PKCS #7

$m = 128b$

x_{n+1}

| 15B | 01 |

| 14B | 02 | 02 |

| 13B | 03 | 03 | 03 |

⋮

$$\boxed{1B}\ \underbrace{\boxed{0F}\ \boxed{0F}\ \dots\ \boxed{0F}}_{15}$$

$$\boxed{0B}\ \underbrace{\boxed{00}\ \boxed{00}\ \dots\ \boxed{00}}_{16}$$

$\longleftarrow K \longrightarrow$

A | E | B

$\cancel{m} \longrightarrow$

$m \to e_K(m) \xrightarrow{e_K(m)} d_K(e_K(m)) = m$

Kryptografia klucza publicznego

Diffie-Hellman | Ellis

Rivest-Shamir-Adleman | Cocks

A | E m | B

K_B^{priv} K_B^{pub}

klucz Alicji

$L \to e_{K_B^{pub}}(L) \longrightarrow d_{K_B^{priv}}(e_{K_B^{pub}}(L)) = L$

znane wszystkim

Bob musi mieć klucz prywatny

funkcja łatwo obliczalna

f. trudno obliczalna (bez znajomości K_B^{priv})

funkcja z zapadką

funkcja jednokierunkowa

?

RSA

p, q - dwie liczby pierwsze (różne)

$n = pq$

$\mathcal{P} = \mathcal{C} = \mathbb{Z}_n = \{0, 1, \dots, n-1\}$

f. Eulera

$\mathcal{K} = \{(n, p, q, a, b) : ab \equiv 1 \pmod{\varphi(n)}\}$

$\varphi(n)$ - liczba liczb od 1 do $n-1$, które są względnie pierwsze z n

$\varphi(10) = \boxed{1 \ 3 \ 7 \ 9}$

$\varphi(10) = 4$

$\boxed{\varphi(p) = p - 1}$

l. pierwsza

$\boxed{\varphi(p^a) = p^a - p^{a-1}}$

$\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$

o ile $NWD(n, m) = 1$

$$\varphi(100) = \varphi(2^2 \cdot 5^2) = \varphi(2^2)\varphi(5^2) =$$
$$= (2^2 - 2^1)(5^2 - 5^1) = 2 \cdot (25 - 5) = \boxed{40}$$

$$n = pq \qquad \varphi(n) = \varphi(pq) = \varphi(p)\varphi(q)$$
$$= (p-1)(q-1)$$

$$ab \equiv 1 \pmod{\varphi(n)} \iff ab \equiv 1 \pmod{(p-1)(q-1)}$$

$$e_K(x) = x^b \bmod n \quad = y$$

b ← K_B^{pub}

$$\boxed{y = x^b \bmod n \qquad x = ?}$$

$$d_K(y) = x^a \bmod n$$

a ← K_B^{priv}

1) Dlaczego deszyfrowanie działa?

$$x \to x^b \bmod n$$

$$\boxed{(x^b)^a \bmod n = x \quad ?}$$

$$ab \equiv 1 \pmod{\varphi(n)}$$
$$ab = 1 + m\varphi(n)$$

$$(x^b)^a \equiv x^{ba} = x^{1+m\varphi(n)} = x \cdot x^{m\varphi(n)} \equiv$$
$$\equiv x \cdot (\underbrace{x^{\varphi(n)}}_{\equiv 1})^m \equiv x \cdot 1 \equiv x \pmod n$$

tw. Eulera: NWD(A,N) = 1, to

$A^{\varphi(N)} \equiv 1 \pmod N$

$\boxed{\text{cn}}$, w przypadku, gdy $NWD(x, n) > 1$.

2) Podział klucza

(n, p, q, a, b)

Alicja, Ewa — (n, b)

Bob — a

3) Jak skonstruować a i b?

b losowe, ale takie, że $NWD(b, \varphi(n)) = 1$

$a = b^{-1} \bmod \varphi(n)$ ← Rozszerzony alg. Euklidesa

$\varphi(n) = (p-1)(q-1)$

$ab \equiv 1 \pmod{\varphi(n)}$